Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

THE
AMERICAN
MATHEMATICAL MONTHLY.

Entered at the Post-office at Springfield, Missouri, as second-class matter.

VOL. XII. APRIL, 1905. No. 4.

APPLICATION OF SEVERAL THEOREMS IN NUMBER THEORY TO GROUP THEORY.

By DR. G. A. MILLER, Stanford University.

Two previous notes (MONTHLY, Vol. 11, p. 129, and Vol. 12, p. 41) were devoted to exhibiting the advantages of employing elementary theorems in group theory in the proof of some of the fundamental theorems of number theory. The present note, on the contrary, aims to translate into the language of group theory several other important theorems of number theory. The object is to make these theorems more available to the student of group theory rather than to emphasize the advantages resulting from the employment of group theory concepts in the study of number theory. As most of the developments relate to ground which is decidedly common to the two subjects it is hoped that some of the results are also useful from the standpoint of number theory.

It is well known that a cyclic substitution of even order generates a group (C) in which half the substitutions are even and the other half are odd. The even substitutions are squares and the odd substitutions are non-squares under C.* As any substitution (s) has the same square as s multiplied by the substitution of order 2 contained in C, it follows that the two square roots of any even substitution are either both odd or both even when the order of C is divisible by 4. When this order is not divisible by 4 one of these square roots is even and the other is odd.

Let C be the group of isomorphisms of the cyclic group of order p, p being any odd prime. With each substitution of C may be associated a number which is congruent (mod p) to the index of the power into which this substitution transforms the operators of the cyclic group of order p. With respect to modulus p these numbers constitute a group which is simply isomorphic with C.[*] If k is any one of these numbers the corresponding substitution is even or odd as $\left(\frac{k}{p}\right)$ is $+1$ or -1; *i. e.* as k is a quadratic residue or quadratic non-residue of p.[†] Even substitutions are sometimes called positive and odd substitutions are called negative. If this is done the Legendre symbol $\left(\frac{k}{p}\right)$ exhibits whether the substitution corresponding to k is positive or negative.

---

*The even substitutions constitute a subgroup whose order is half the order of C.

The preceding developments remain unchanged if C is regarded as the group of isomorphisms of the cyclic group of order p^α, as should be the case since a quadratic residue of p is also a quadratic residue of p^α and vice versa. That is, if we associate with the substitutions of the cyclic group of order $p^{\alpha-1}(p-1)$ the indices (mod p^α) of the powers into which these substitutions transform the operators of a cyclic group of order p^α, each substitution is positive or negative as $\left(\frac{k}{p^\alpha}\right)$ is $+1$ or -1, k being the corresponding index. From the preceding paragraph it follows that just half of the first $m(p-1)$ natural numbers which are prime to p are quadratic residues of p while the other half are quadratic non-residues, m being arbitrary. From the present paragraph it is clear that just half of the first $p^{\alpha-1}(p-1)$ numbers which are prime to p are quadratic residues of p^α. As a quadratic residue of p^α is also a quadratic residue of p, the last two sentences furnish a direct proof of the theorem that a quadratic residue of p is also a quadratic residue of p^α.[‡]

The main results of the last two paragraphs may also be stated as follows: *If the* $p^{\alpha-1}(p-1)$ *numbers which are less than* p^α *and prime to* p *are arranged in any order whatsoever and are then multiplied by any number* (k) *prime to* p, *the products* (*modulo* p^α) *give a rearrangement of these numbers which represents a substitution of degree* $p^{\alpha-1}(p-1)$, *whenever* k *is not identical to* 1 *mod* p^α. *This substitution is positive or negative as* $\left(\frac{k}{p}\right)$ *is* $+1$ *or* -1. For the case when $\alpha=1$ this theorem was proved by Zolotareff and is of fundamental importance in his proof of the law of quadratic reciprocity by means of substitution theory.[§]

If p and q are distinct odd primes, the cyclic group (C) of order $p^\alpha q^\beta$ may be represented as an intransitive substitution group of degree $p^\alpha + q^\beta$ and this is the smallest number of letters on which it can be represented. Suppose that C is represented in this way. The group of isomorphisms (I) of C is the direct product of the two cyclic groups of orders $p^{\alpha-1}(p-1)$, $q^{\beta-1}(q-1)$, respectively, and may be represented as an intransitive substitution group involving two systems of intransitivity of degrees $p^{\alpha-1}(p-1)$ and $q^{\beta-1}(q-1)$, respectively.

---

[*] *Annals of Mathematics*, Vol. 2 (1901), p. 78.

[†] Since the numbers are squares whenever the corresponding substitutions are squares.

[‡] This result can also be seen directly from the substitutions of the given cyclic group of order $p^{\alpha-1}(p-1)$.

[§] Zolotareff, *Nouvelles Annales*, Vol. 11 (1872), p. 354.

We may again associate with each substitution of I the index (modulo $p^\alpha q^\beta$) of the power into which the substitution transforms all the substitutions of C. If this is done Legendre's law of quadratic reciprocity says that the substitution which corresponds to $k \equiv p+q$ modulo $p^\alpha q^\beta$ is positive unless p and q are both of the form $4n+3$. It is clear that the positive substitutions of I correspond to numbers which are either quadratic residues of both p and q, or quadratic non-residues of both p and q. The negative substitutions of I correspond to numbers which are quadratic residues of only one of the two numbers p, q.

In abstract group theory the following direct application of the law of quadratic reciprocity is evident from the preceding developments. If the group of isomorphisms I of the cyclic group of order p^α is represented as a number group modulo p^α all the numbers which are in the subgroup of order $\frac{p^{\alpha-1}(p-1)}{2}$ are quadratic residues of p while the remaining numbers are non-residues. All the numbers of I may be represented by primes in an infinite number of ways since they are only determined with respect to modulus p^α. Legendre's law of quadratic reciprocity states that if q is any prime in the subgroup of I whose order is $\frac{p^{\alpha-1}(p-1)}{2}$ then will the numbers which are congruent to p mod q be in the subgroup of order $\frac{q^{\beta-1}(q-1)}{2}$ of the group of isomorphisms of the cyclic group of order q^β, unless both p and q are of the form $4n+3$.

Since the subgroup of order p^{α_1}, $\alpha_1 < \alpha$, contained in I is composed of the numbers which are congruent to 1 modulo $p^{\alpha-\alpha_1}$, it follows that the subgroup of order $\frac{p^{\alpha_1}(p-1)}{d}$ contained in I is composed of the numbers which are congruent modulo $p^{\alpha-\alpha_1}$ to the numbers of the subgroup of order $\frac{p-1}{d}$. When $d=2$ the latter numbers are the quadratic residues of p modulo p. If we multiply these numbers by the numbers in the subgroup of order p^{α_1} the products are still quadratic residues of p. By making $\alpha_1 = \alpha - 1$ we have another proof of the theorem that a quadratic residue of p if also a quadratic residue of p^α. Another particular case is that *every subgroup of I whose order is divisible by $p^{\alpha-1}$ includes the numbers which are congruent to any of its numbers modulo p.*

While we know some of the properties of the numbers in the subgroups of I, little is known in reference to what particular numbers occur in these subgroups. It is evident that $p^\alpha - 1$ occurs in every subgroup of even order. That is, when the group constituted by the quadratic residues of p^α is of even order, -1 is a quadratic residue of p and vice versa. This follows directly from the fact that -1 corresponds to the operator of order 2 in I. The numbers 1 and -1 are the only ones whose orders are independent of the value of the modulus.

As has been observed above the numbers whose orders are given powers of p can also be directly written down. The determination of the numbers whose orders divide $p-1$ presents difficulties which have not yet been surmounted. If we knew the latter numbers and their orders, we would know the orders of all the numbers, since the order of the product of two such numbers is the product of their orders. In the case when $p=3$, the operators whose orders divide $p-1$ are 1 and p^a-1. Hence, in this case, the order of every number is known. In particular, the primitive roots of p^a are the products of p^a-1 into the numbers of the form $1+kp$ (k being prime to p), as is well known.

Even the number 2 presents difficulties which have not been overcome. That is, we do not know the order of the operator which transforms each operator of C into its square. The well known number theory results along this line; that is, those which relate to the quadratic character of 2, may be stated in group theory language as follows: In the number group formed by the natural numbers which are prime to p and less than p^a, the order of 2 divides $\frac{p^{a-1}(p-1)}{2}$ only when p is of the form $8n\pm1$. When p is not of this form the order of 2 must involve the highest power of 2 contained in $p-1$.

A SHORT PROOF FOR THE NUMBER OF TERMS IN A DETERMINANT WHICH ARE INDEPENDENT OF THE ELEMENTS OF THE PRINCIPAL DIAGONAL.

By ORLANDO S. STETSON, Syracuse University.

The problem of finding the number of terms, $\varphi(n)$, in the given determinant which are independent of the elements of the principal diagonal may be reduced to the question of finding the number of terms in the expansion of the *invertebrate* determinant Δ_n (second formula for $k=n$, MONTHLY, 1904, page 167).

Hence

$$\varphi(n)=n!-n(n-1)!+\frac{n(n-1)}{1.2}(n-2)!-\frac{n(n-1)(n-2)}{1.2.3}(n-3)!$$

$$+\ldots\ldots+(-1)^{n-1}\frac{n(n-1)(n-2)\ldots\ldots3.2}{1.2.3\ldots\ldots(n-1)}(1)!+(-1)^n\frac{n(n-1)(n-2)\ldots\ldots3.2.1}{1.2.3\ldots\ldots n}$$

Removing from each of the terms the factor $n!$ and noticing that the first two terms are equal but opposite in sign, we have

$$\varphi(n)=n!\left[\frac{1}{1.2}-\frac{1}{1.2.3}+\frac{1}{1.2.3.4}-\ldots\ldots+(-1)^n\frac{1}{1.2.3\ldots\ldots n}\right].$$